PCT/JP00/00475

09/890286

JP00/475

28.01.00

REC'D 17 MAR 2000

WIPO PCT

EJU

日本国特許庁
PATENT OFFICE JAPANESE GOVERNMENT

#3

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: １９９９年　８月２６日

出願番号
Application Number: 平成１１年特許願第２３９１７７号

出願人
Applicant (s): 株式会社日立製作所

２０００年　３月　３日

特許庁長官
Commissioner,
Patent Office 近藤隆彦

出証番号　出証特２０００－３０１１６８０

【書類名】　特許願

【整理番号】　K99009761

【提出日】　平成11年 8月26日

【特記事項】　特許法第３０条第１項の規定の適用を受けようとする特許出願

【あて先】　特許庁長官殿

【国際特許分類】　G09C 1/00

【請求項の数】　17

【発明者】

【住所又は居所】　神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所　システム開発研究所内

【氏名】　西岡　玄次

【特許出願人】

【識別番号】　000005108

【氏名又は名称】　株式会社日立製作所

【代理人】

【識別番号】　100075096

【弁理士】

【氏名又は名称】　作田　康夫

【手数料の表示】

【予納台帳番号】　013088

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　選択暗号文攻撃に強い公開鍵暗号方法及び装置

【特許請求の範囲】

【請求項１】

送信者は，受信者の公開鍵を用いて送信データを暗号化する公開鍵暗号方法であって，

鍵生成のステップとして，

【数１】

- G：有限アーベル群
- $s \in \mathbf{Z}$，　$gh^s = 1 \ (\in H)$
- $\alpha^{-1} \in \mathbf{Z}$

・・・(数1)

なる秘密鍵（G,s,α^{-1}）を作成し（但し，α^{-1}はHの濃度を法とする環におけるαの逆元），さらに，

【数２】

- H：Gの部分群
- $g, h \in G$
- $\alpha \in \mathbf{Z}$

・・・(数2)

なる公開鍵（H,g,h,α）を作成し（但し，kはpqのビット長），

（１）送信者は，平文m(∈H)および乱数rに対して，

【数３】

$$C = m^{\alpha} g^{r}, \quad D = h^{r} \quad (\in G)$$

・・・(数3)

を計算し，さらに暗号文から平文が一意的に復号化されるための付加情報aを計算し，(C,D,a)を暗号文として前記受信者に送信し，

（２）前記受信者は，自身の秘密鍵（H,s,α^{-1}）を用いて，暗号文(C,D,a)から

，

【数４】

$$\hat{m} = (CD^{s})^{\alpha^{-1}} \quad (\in H) \qquad \cdots (数4)$$

を計算し，さらに付加情報aから元の平文mを計算する

ことを特徴とする公開鍵暗号方法。

【請求項２】

請求項１において，前記公開情報（G,g,h,α）は，前記受信者が生成し，公開することを特徴とする公開鍵暗号方法。

【請求項３】

請求項１および２において，

ランダム関数Ｈを公開するステップを備え，

送信者が作成した平文に対して，乱数情報とランダム関数Ｈの結果を排他的論理和およびデータの連接による演算を行うステップを備え，

さらに，該演算を行った結果を，請求項１における平文ｍの箇所，または，乱数ｒの箇所に置き換え，請求項１における公開鍵暗号化方法の手順により暗号化する

ことを特徴とする公開鍵暗号における暗号化方法。

【請求項４】

請求項３の方法により暗号化した暗号文を復号化する方法において，

請求項１の公開鍵暗号方法による復号化手順を行うステップを備え，

さらに，請求項３において行われた該演算（平文ｍ'に対して乱数情報とランダム関数Ｈの結果を排他的論理和およびデータの連接による演算）の手順の正当性を確かめるステップを備え，

その後，復号化結果を出力する

ことを特徴とする公開鍵暗号における復号化方法。

【請求項５】

送信者は，受信者の公開鍵を用いて送信データを暗号化する公開鍵暗号方法であって，

鍵生成のステップとして，

【数５】

- p, q：素数，　$p \equiv 3 \pmod 4$, $q \equiv 3 \pmod 4$
- $s \in \mathbb{Z}$,　$gh^s \equiv 1 \pmod{pq}$　　・・・(数5)
- $\beta \in \mathbb{Z}$,　$\alpha\beta \equiv 1 \pmod{\mathrm{lcm}(p-1, q-1)}$

なる秘密鍵（p,q,s,β）を作成し，さらに，

【数６】

- $\alpha, g, h, k, l \in \mathbb{Z}$　$(0 < g, h < n)$
- $n = p^d q$　　(d は奇数)　　・・・(数6)

なる公開鍵（n,g,h,k,l,α）を作成し（但し，kはpqのビット長），

（１）送信者は，平文m$(0<m<2^{k-2})$および乱数r（0≦r≦l）に対して，

【数７】

$$C = m^{2\alpha} g^{r'} \bmod n, \quad D = h^{r'} \bmod n \qquad \cdots (数7)$$

を計算し，さらにJacobi記号a=(m/n)を計算し，(C,D,a)を暗号文として前記受信者に送信し，

（２）前記受信者は，自身の秘密鍵（p,q,s,β）を用いて，暗号文(C,D,a)から

，

【数８】

$$\begin{aligned} m_{1,p} &= (CD^s)^{\frac{\beta(p+1)}{4}} \bmod p, \\ m_{1,q} &= (CD^s)^{\frac{\beta(q+1)}{4}} \bmod q \end{aligned} \qquad \cdots (数8)$$

を計算し，$\phi(m_{1,p}, m_{1,q})$, $\phi(-m_{1,p}, m_{1,q})$, $\phi(m_{1,p}, -m_{1,q})$, $\phi(-m_{1,p}, -m_{1,q})$のうち，(x/n)=aかつ$0<x<2^{k-2}$を満たすxを平文mとする（但し，ϕは中国人の剰余定理によるZ/(p)×Z/(q)からZ/(pq)への環同型写像を表す。），

ことを特徴とする公開鍵暗号方法。

【請求項６】

請求項５において，前記公開情報（n,g,h,k,l,α）は，前記受信者が生成し，公開することを特徴とする公開鍵暗号方法。

【請求項７】

送信者は，受信者の公開鍵を用いて送信データを暗号化する公開鍵暗号方法であって，

鍵生成のステップとして，

【数９】

- p, q : 素数, $p \equiv 3 \pmod 4$, $q \equiv 3 \pmod 4$
- $\beta \in \mathbb{Z}$, $\alpha\beta \equiv 1 \pmod{\mathrm{lcm}(p-1, q-1)}$

・・・(数9)

なる秘密鍵（p,q,β）を作成し，さらに，

【数１０】

- $\alpha, k \in \mathbb{Z}$
- $n = p^d q$ (d は奇数)

・・・(数１０)

なる公開鍵（n,k,α）を作成し（但し，kはpqのビット長），

（１）送信者は，平文m（$0<m<2^{n-k1}$）に対して，

【数１１】

$$m_1 = m0^{k_1} \oplus G(r) \,||\, r \oplus H(m0^{k_1} \oplus G(r)) \qquad (0 < m_1 < 2^{k-2})$$

・・・(数１１)

を計算し（但し，$G: \{0,1\}^{k0} \rightarrow \{0,1\}^{n}$, $H: \{0,1\}^{n} \rightarrow \{0,1\}^{k0}$, は適当なランダム関数であり，$k=n+k_0+2$とする。），さらにJacobi記号$a=(m_1/n)$，および，

【数１２】

$$C = m_1^{2\alpha} \bmod n,$$

・・・(数１２)

を計算し，(C,a)を暗号文として前記受信者に送信し，

（２）前記受信者は，自身の秘密鍵（p,q,β）を用いて，暗号文(C,a)から，

【数１３】

$$m_{1,p} = C^{\frac{\beta(p+1)}{4}} \bmod p, \qquad \cdots(数13)$$
$$m_{1,q} = C^{\frac{\beta(q+1)}{4}} \bmod q$$

を計算し，$\phi(m_{1,p},m_{1,q})$，$\phi(-m_{1,p},m_{1,q})$，$\phi(m_{1,p},-m_{1,q})$，$\phi(-m_{1,p},-m_{1,q})$のうち，(x/n)=aかつ$0<x<2^{k-2}$を満たすxをm'_1として計算し（但し，ϕは中国人の剰余定理によるZ/(p)×Z/(q)からZ/(pq)への環同型写像を表す。），

さらに，$m'_1=s'||t'$（s'はm'_1の上位nビット，t'は下位k_0ビット）に対して，

【数１４】

$$m' = \begin{cases} [s' \oplus G(t' \oplus H(s'))]^{n-k_1} & \text{if } [s' \oplus G(t' \oplus H(s'))]_{k_1} = 0^{k_1} \\ * & \text{otherwise} \end{cases} \qquad \cdots(数14)$$

を計算し，これを復号化結果とする（但し，$[a]^n$および$[a]_n$はそれぞれaの上位および下位nビットを表す。）

ことを特徴とする公開鍵暗号方法。

【請求項８】

請求項７において，前記公開情報（n,k,α）は，前記受信者が生成し，公開することを特徴とする公開鍵暗号方法。

【請求項９】

送信者は，受信者の公開鍵を用いて送信データを暗号化する公開鍵暗号方法であって，

鍵生成のステップとして，

【数１５】

- p, q：素数，$p \equiv 3 \pmod 4$, $q \equiv 3 \pmod 4$
- $s \in \mathbb{Z}$, $gh^s \equiv 1 \pmod{pq}$ $\qquad \cdots(数15)$
- $\beta \in \mathbb{Z}$,, $\alpha\beta \equiv 1 \pmod{\mathrm{lcm}(p-1, q-1)}$

なる秘密鍵（p,q,s,β）を作成し，さらに，

【数１６】

- $\alpha, g, h, k, l \in \mathbb{Z} \quad (0 < g, h < n)$ ・・・(数16)
- $n = p^d q \quad (d$ は奇数$)$

なる公開鍵（n,g,h,k,l,α）を作成し（但し，kはpqのビット長），

（１）送信者は，平文m（$0<m<2^{n-k1}$）に対して，

【数１７】

$$m_1 = m0^{k_1} \oplus G(r) \,||\, r \oplus H(m0^{k_1} \oplus G(r)) \quad (0 < m_1 < 2^{k-2}) \qquad \cdots(数17)$$

を計算し（但し，$G: \{0,1\}^{k0} \rightarrow \{0,1\}^{n}$，$H: \{0,1\}^{n} \rightarrow \{0,1\}^{k0}$，は適当なランダム関数であり，$k=n+k_0+2$とする。），さらにJacobi記号$a=(m_1/n)$，および，

【数１８】

$$C = m_1{}^{2\alpha} g^{r'} \bmod n, \quad D = h^{r'} \bmod n \qquad \cdots(数18)$$

を計算し，(C,D,a)を暗号文として前記受信者に送信し，

（２）前記受信者は，自身の秘密鍵（p,q,s,β）を用いて，暗号文(C,D,a)から

，

【数１９】

$$m_{1,p} = (CD^s)^{\frac{\beta(p+1)}{4}} \bmod p, \qquad \cdots(数19)$$
$$m_{1,q} = (CD^s)^{\frac{\beta(q+1)}{4}} \bmod q$$

を計算し，$\phi(m_{1,p}, m_{1,q})$，$\phi(-m_{1,p}, m_{1,q})$，$\phi(m_{1,p}, -m_{1,q})$，$\phi(-m_{1,p}, -m_{1,q})$のうち，(x/n)=aかつ$0<x<2^{k-2}$を満たすxをm'_1として計算し（但し，φは中国人の剰余定理によるZ/(p)×Z/(q)からZ/(pq)への環同型写像を表す。），

さらに，$m'_1 = s' || t'$（s'はm'_1の上位nビット，t'は下位k_0ビット）に対して，

【数２０】

$$m' = \begin{cases} [s' \oplus G(t' \oplus H(s'))]^{n-k_1} & \text{if } [s' \oplus G(t' \oplus H(s'))]_{k_1} = 0^{k_1} \\ * & \text{otherwise} \end{cases} \quad \cdots (数20)$$

を計算し，これを復号化結果とする（但し，$[a]^n$および$[a]_n$はそれぞれaの上位および下位nビットを表す。）

ことを特徴とする公開鍵暗号方法。

【請求項１０】

請求項９において，前記公開情報（n,g,h,k,α）は，前記受信者が生成し，公開することを特徴とする公開鍵暗号方法。

【請求項１１】

送信者は，受信者の公開鍵を用いて送信データを暗号化する公開鍵暗号方法であって，

鍵生成のステップとして，

【数２１】

- p, q：素数，$p \equiv 3 \pmod 4$, $q \equiv 3 \pmod 4$
- $s \in \mathbb{Z}$, $gh^s \equiv 1 \pmod{pq}$ $\cdots (数21)$
- $\beta \in \mathbb{Z}$, $\alpha\beta \equiv 1 \pmod{\mathrm{lcm}(p-1, q-1)}$

なる秘密鍵（p,q,s,β）を作成し，さらに，

【数２２】

- $\alpha, g, h, k, l \in \mathbb{Z} \quad (0 < g, h < n)$ $\cdots (数22)$
- $n = p^d q \quad (d$ は奇数$)$

なる公開鍵（n,g,h,k,l,α）を作成し（但し，kはpqのビット長），

（１）送信者は，平文m（$0<m<2^n$）に対して，

【数２３】

$$m_1 = m \oplus G(r) \,||\, r \oplus H(m \oplus G(r)) \quad (0 < m_1 < 2^{k-2}) \qquad \cdots (数23)$$

を計算し（但し，G: $\{0,1\}^{k0} \rightarrow \{0,1\}^{n}$，H: $\{0,1\}^{n} \rightarrow \{0,1\}^{k0}$，は適当なランダム関数であり，$k=n+k_0+2$とする。），さらにJacobi記号$a=(m_1/n)$，および，

【数２４】

$$C = m_1^{2\alpha} g^{F(m_1)} \bmod n, \quad D = h^{F(m_1)} \bmod n \qquad \cdots (数24)$$

を計算し（但し，F: $\{0,1\}^{n+k0} \rightarrow \{0,1\}^{l}$は適当なランダム関数），(C,D,a)を暗号文として前記受信者に送信し，

（２）前記受信者は，自身の秘密鍵（p,q,s,β）を用いて，暗号文(C,D,a)から

，

【数２５】

$$\begin{aligned} m_{1,p} &= (CD^s)^{\frac{\beta(p+1)}{4}} \bmod p, \\ m_{1,q} &= (CD^s)^{\frac{\beta(q+1)}{4}} \bmod q \end{aligned} \qquad \cdots (数25)$$

を計算し，$\phi(m_{1,p}, m_{1,q})$，$\phi(-m_{1,p}, m_{1,q})$，$\phi(m_{1,p}, -m_{1,q})$，$\phi(-m_{1,p}, -m_{1,q})$のうち，(x/n)=aかつ$0<x<2^{k-2}$を満たすxをm'_1として計算し（但し，ϕは中国人の剰余定理によるZ/(p)×Z/(q)からZ/(pq)への環同型写像を表す。），

さらに，$m'_1 = s' || t'$（s'はm'_1の上位nビット，t'は下位k_0ビット）に対して，

【数２６】

$$m' = \begin{cases} s' \oplus G(t' \oplus H(s')) & \text{if } (C,D) = (C',D') \\ * & \text{otherwise} \end{cases} \qquad \cdots (数26)$$

を計算し，これを復号化結果とする（但し，

【数２７】

$$C' = m_1'^2 g^{F(m_1')} \bmod n, \quad D' = h^{F(m_1')} \bmod n \qquad \cdots (数27)$$

であり，$[a]^n$および$[a]_n$はそれぞれaの上位および下位nビットを表す。）

ことを特徴とする公開鍵暗号方法。

【請求項１２】

請求項１１において，前記公開情報（n,g,h,k,α）は，前記受信者が生成し，公開することを特徴とする公開鍵暗号方法。

【請求項１３】

送信者は，受信者の公開鍵を用いて送信データを暗号化する公開鍵暗号方法であって，

鍵生成のステップとして，

【数２８】

- p, q：素数，$p \equiv 3 \pmod 4$, $q \equiv 3 \pmod 4$
- $s \in \mathbb{Z}$, $gh^s \equiv 1 \pmod{pq}$
- $\beta \in \mathbb{Z}$, $\alpha\beta \equiv 1 \pmod{\mathrm{lcm}(p-1, q-1)}$

$\cdots (数28)$

なる秘密鍵（p,q,s,β）を作成し，さらに，

【数２９】

- $\alpha, g, h, k, l \in \mathbb{Z} \quad (0 < g, h < n)$
- $n = p^d q \qquad (d$ は奇数$)$

$\cdots (数29)$

なる公開鍵（n,g,h,k,l,α）を作成し（但し，kはpqのビット長），

（１）送信者は，平文m（$0<m<2^n$）に対して，乱数r（$0<r<2^{k0}$）を選び，

【数３０】

$$m_1 = m \| r \qquad \cdots(数30)$$

を計算し（但し，F: $\{0,1\}^{n+k0} \rightarrow \{0,1\}^{l}$は適当なランダム関数であり，$k=n+k_0+2$とする。），さらにJacobi記号$a=(m_1/n)$，および，

【数３１】

$$C = m_1^{2\alpha} g^{F(m_1)} \bmod n, \quad D = h^{F(m_1)} \bmod n \qquad \cdots(数31)$$

を計算し，(C,D,a)を暗号文として前記受信者に送信し，

（２）前記受信者は，自身の秘密鍵（p,q,s,β）を用いて，暗号文(C,D,a)から

【数３２】

$$\begin{aligned} m_{1,p} &= (CD^s)^{\frac{\beta(p+1)}{4}} \bmod p, \\ m_{1,q} &= (CD^s)^{\frac{\beta(q+1)}{4}} \bmod q \end{aligned} \qquad \cdots(数32)$$

を計算し，$\phi(m_{1,p}, m_{1,q})$, $\phi(-m_{1,p}, m_{1,q})$, $\phi(m_{1,p}, -m_{1,q})$, $\phi(-m_{1,p}, -m_{1,q})$のうち，(x/n)=aかつ$0<x<2^{k-2}$を満たすxをm'_1として計算し（但し，ϕは中国人の剰余定理によるZ/(p)×Z/(q)からZ/(pq)への環同型写像を表す。），

さらに，

【数３３】

$$m' = \begin{cases} [m'_1]^{k_0} & \text{if } (C,D) = (C',D') \\ * & \text{otherwise} \end{cases} \qquad \cdots(数33)$$

を計算し，これを復号化結果とする（但し，

【数３４】

$$C' = m_1'^2 g^{F(m_1')} \bmod n, \quad D' = h^{F(m_1')} \bmod n \qquad \cdots (数34)$$

であり，$[a]^n$および$[a]_n$はそれぞれaの上位および下位nビットを表す。）

ことを特徴とする公開鍵暗号方法。

【請求項１４】

請求項１３において，前記公開情報（n,g,h,k,α）は，前記受信者が生成し，公開することを特徴とする公開鍵暗号方法。

【請求項１５】

請求項７から請求項１４において，

d（d≧１）の値を可変とする

ことを特徴とする公開鍵暗号方法および鍵共有方法。

【請求項１６】

請求項９および請求項１０において，暗号化処理のとき，

【数３５】

$$g^{r'} \bmod n, \quad h^{r'} \bmod n \qquad \cdots (数35)$$

の計算を前処理にて行うステップを備える

ことを特徴とする公開鍵暗号方法。

【請求項１７】

請求項１１から請求項１４において，復号化処理のとき，

受信者側は，

【数３６】

$$C_p' = m_1'^{2\alpha} g^{F(m_1')} \bmod p^d, \quad C_q' = m_1'^2 g^{F(m_1')} \bmod q$$
$$D_p' = h^{F(m_1')} \bmod p^d, \quad D_q' = h^{F(m_1')} \bmod q \qquad \cdots (数36)$$

を計算し，さらに

【数３７】

$$C \equiv C'_p \pmod{p^d}, \quad C \equiv C'_q \pmod{q}, \quad D \equiv D'_p \pmod{p^d}, \quad D \equiv D'_q \pmod{q} \qquad \cdots (数37)$$

により，(C,D)=(C',D')を検査するステップを備える

ことを特徴とする公開鍵暗号方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は，公開鍵暗号を用いた暗号通信方法および装置に関する。

【０００２】

【従来の技術】

現在まで，様々な公開鍵暗号方式が提案されている。なかでも，文献１「R.L. Rivest,A.Shamir,L.Adleman.:A method for obtaining digital signatures and public-key cryptosystems, Commun. of the ACM, Vol.21, No.2, pp.120-126, 1987.」に掲載されている方法が最も有名であり，最も実用化されている公開鍵暗号である。

【０００３】

その他には，文献２「T.ElGamal.:A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms, IEEE Trans. On Information Theory, IT-31, 4, pp.469-472(1985)」に記載されている暗号方法，文献３「M.O.Rabin.: Digital Signatures and Public-Key Encryptions as Intractable as Factorization, MIT, Technical Report, MIT/LCS/TR-212 (1979)」に記載されている暗号方法，文献４「V.S.Miller.:Use of Elliptic Curves in Cryptography, Proc. of Crypto'85, LNCS 218, Springer-Verlag, pp.417-426 (1985)」，文献５「N.Koblitz.: Elliptic Curve Cryptosystems, Math. Comp., 48, 177, pp.203-209 (1987)」等に記載の楕円曲線を用いた方法，文献６「S.Goldwasser and S.Micali.: Probabilistic Encryption, JCSS, 28, 2, pp.270-299 (1984)」に

記載されている暗号方法，文献７「M.Blum and S.Goldwasser.: An Efficient probabilistic public-key encryption scheme which hides all partial information, Proc. of Crypto'84, LNCS 196, Springer-Verlag, pp.289-299 (1985)」に記載されている暗号方法，文献８「S.Goldwasser and M.Bellare.: Lecture Notes on Cryptography, http:/www-cse.ucsd.edu/users/mihir/ (1997)」に記載されている暗号方法，文献９「R.Cramer and V.Shoup.: A Practical Public Key Cryptosystem Provably Secure against Adaptive Chosen Ciphertext Attack, Proc. of Crypto98, LNCS, Springer-Verlag, pp.13-25 (1998)」に記載されている暗号方法，文献１０「T.Okamoto and S.Uchiyama,.A New Public-Key Cryptosystem as Secure as Factoring, Proc. of Eurocrypt'98, LNCS, Springer Verlag, pp.308-318 (1998)」に記載されている暗号方法，などが知られている。

【０００４】

特に，最近では，安全性の証明が可能な公開鍵暗号が注目されている。ここで，安全性が証明できるとは，「ある攻撃（受動的攻撃または能動的攻撃）に対してその公開鍵暗号が安全（強秘匿性，頑強性，等）であること」と，「ある数論的問題（素因数分解問題，Diffie-Hellman決定問題，等）が困難であること」の等価性を証明できる公開鍵暗号のことである。

【０００５】

Bellareらは，文献１１「M.Bellare, A.Desai, D.Pointcheval and P.Rogaway,.Relations Among Notions of Security for Public-Key Encryption Schemes, Proc. of Crypto'98, LNCS, Springer Verlag」で，IND-CCA2（適応的選択暗号文攻撃に対して強秘匿であること）とNM-CCA2（適応的選択暗号文攻撃に対して頑強であること）の等価性を示し，この条件を満たす公開鍵暗号が最も安全であると考えられている。

【０００６】

例えば，Bellareらは，文献１２「M.Bellare and P.Rogaway,.Optimal Asymmetric Encryption How to Encrypt with RSA, Proc. of Eurocrypt'94, LNCS, Springer Verlag」で，一般的な落とし戸付き置換をIND-CCA2に変換する方法につ

いて提案し，さらにＲＳＡ暗号をこの方法により変換した公開鍵暗号方式（ＯＡＥＰ）を提案している。ＯＡＥＰはランダムオラクルモデル（理想的なランダム関数へのアクセスが許される）の上で安全性が証明でき，実用のシステムではこの部分が適当なハッシュ関数に置き換えられるため，実用のシステムにおいては安全性は証明できないことになる。しかし，同様の安全性を得られるものと予想され，また，同じくIND-CCA2であることが証明されている上記文献９の方法（この方法は理想的なランダム関数を前提としない）等に比べ，効率性が優れる等の特徴を持つ。

【０００７】

【発明が解決しようとする課題】

上記「従来の技術」で述べたように，現在では，IND-CCA2（適応的選択暗号文攻撃に対して強秘匿）またはNM-CCA2（適応的選択暗号文攻撃に対して頑強）である公開鍵暗号が最も安全であると考えられている。

【０００８】

本発明の目的は，選択平文攻撃に対して一方向（OW-CPA）であり，かつ選択平文攻撃に対して強秘匿（IND-CPA）である公開鍵暗号方法を提供することである。

【０００９】

本発明の更なる目的は，従来技術であるOAEPなどに比べて，より困難な問題の計算量的複雑さを前提としてIND-CCA2（またはNM-CCA2）であることが証明できる公開鍵暗号方法を提供することである。

【００１０】

また，本発明の他の目的は，送信データを暗号化する際の計算および暗号化データを復号化する際の計算の負荷が小さく，携帯型情報処理機器など計算能力が限られた装置であっても高速処理が可能な，公開鍵を用いた暗号化方法と復号化方法と，それを用いた鍵配送方法や鍵共有方法，さらには，これらの方法を実行するプログラム，装置またはシステムを提供することである。

【００１１】

【課題を解決するための手段】

上記目的を達成するため，本発明は以下のように構成する。

【００１２】

（１）選択平文攻撃に対する一方向性（OW-CPA）を素因数分解問題よりも困難な問題の難しさを前提として保証可能な公開鍵暗号方法に対して，平文に乱数情報と（理想的）ランダム関数へのアクセスの結果から排他的論理和および連接（データの単純な接続）の変換（以下，変換Conと呼ぶ）を行う。これにより，適応的選択暗号文攻撃に対する強秘匿性（IND-CCA2）を，素因数分解問題の困難性以上の暗号学的仮定により保証する。すなわち，本発明が提供する暗号化方法への安全性を，従来方式よりもさらに高い立場にて保証する。

【００１３】

これにより，適応的選択暗号文攻撃に対する強秘匿性（IND-CCA2）を，素因数分解問題の困難性（または，それ以上）の暗号学的仮定により保証することができる。すなわち，本発明が提供する暗号化方法への安全性を，従来方式よりもさらに高い立場にて保証する。

【００１４】

（２）変換Conにおいては，排他的論理和と連接の組み合わせからなる。変換Conは高速な処理が可能であり，変換Conを行った後の本発明による公開鍵暗号方法は変換を行う前の公開鍵暗号方法における高速な暗復号化処理とほぼ同等の処理が可能となる。

【００１５】

（３）暗号化の過程において，確率的な情報を用いた処理を施す。これにより，暗号化する平文に対して確率的情報を挿入する必要がない。すなわち，本発明が提供する暗号化方法は，同一の平文であっても暗号文の値が変化する確率暗号である。

【００１６】

（４）送信データを暗号化する際の計算および暗号化データを復号化する際の計算の双方の負荷が少なく，高速な暗復号化処理が可能であるように構成する。

【００１７】

すなわち，本発明は，送信者が，受信者の公開鍵を用いて送信データを暗号化する公開鍵暗号方法であって，

鍵生成のステップとして，

【００１８】

【数３８】

- G：有限アーベル群
- $s \in \mathbf{Z}$，　$gh^s = 1 \ (\in H)$　　・・・(数３８)
- $\alpha^{-1} \in \mathbf{Z}$

【００１９】

なる秘密鍵（G,s,α^{-1}）を作成し（但し，α^{-1}はHの濃度を法とする環におけるαの逆元），さらに，

【００２０】

【数３９】

- H：Gの部分群
- $g,h \in G$　　・・・(数３９)
- $\alpha \in \mathbf{Z}$

【００２１】

なる公開鍵（H,g,h,α）を作成し（但し，kはpqのビット長），

（１）送信者は，平文m(∈H)および乱数rに対して，

【００２２】

【数４０】

$$C = m^{\alpha} g^{r}, \quad D = h^{r} \quad (\in G) \qquad \cdots (数４０)$$

【００２３】

を計算し，さらに暗号文から平文が一意的に復号化されるための付加情報aを計算し，(C,D,a)を暗号文として前記受信者に送信し，

（２）前記受信者は，自身の秘密鍵（H,s,α^{-1}）を用いて，暗号文(C,D,a)から

，

【００２４】

【数４１】

$$\tilde{m} = (CD^{s})^{\alpha^{-1}} \quad (\in H) \qquad \cdots (数41)$$

【００２５】

を計算し，さらに付加情報aから元の平文mを計算することを特徴とするものである。

【００２６】

本発明の公開鍵暗号方法は，さらに，前記公開情報（G,g,h,α）は，前記受信者が生成し，公開することを特徴とするものである。

【００２７】

本発明の公開鍵暗号方法は，さらに，ランダム関数Hを公開するステップを備え，

送信者が作成した平文に対して，乱数情報とランダム関数Hの結果を排他的論理和およびデータの連接による演算を行うステップを備え，

さらに，該演算を行った結果を，上記公開鍵暗号化方法おける平文mの箇所，または，乱数rの箇所に置き換え，上記公開鍵暗号化方法の手順により暗号化することを特徴とするものである。

【００２８】

本発明は，さらに，上記公開鍵暗号方法により暗号化した暗号文を復号化する方法において，

さらに，上記公開鍵暗号方法において行われた該演算（平文m'に対して乱数情報とランダム関数Hの結果を排他的論理和およびデータの連接による演算）の手順の正当性を確かめるステップを備え，

その後，復号化結果を出力することを特徴とするものである。

【００２９】

より具体的には，

[鍵生成]

【００３０】

【数４２】

- p, q : 素数, $p \equiv 3 \pmod 4$, $q \equiv 3 \pmod 4$
- $s \in \mathbb{Z}$, $gh^s \equiv 1 \pmod{pq}$ ・・・(数42)
- $\beta \in \mathbb{Z}$, $\alpha\beta \equiv 1 \pmod{\mathrm{lcm}(p-1, q-1)}$

【００３１】

なる秘密鍵（p,q,s,β）を作成し，さらに，

【００３２】

【数４３】

- $\alpha, g, h, k, l \in \mathbb{Z}$ $(0 < g, h < n)$
- $n = p^d q$ (d は奇数) ・・・(数43)

【００３３】

なる公開鍵（n,g,h,k,l,α）を作成し（但し，kはpqのビット長）。

【００３４】

[暗号化]

（１）送信者は，平文m（$0<m<2^{n-k1}$）に対して，

【００３５】

【数４４】

$$m_1 = m0^{k_1} \oplus G(r) \,\|\, r \oplus H(m0^{k_1} \oplus G(r)) \qquad (0 < m_1 < 2^{k-2}) \qquad \cdots (数44)$$

【００３６】

を計算し（但し，$G: \{0,1\}^{k0} \rightarrow \{0,1\}^{n}$, $H: \{0,1\}^{n} \rightarrow \{0,1\}^{k0}$, は適当なランダム関

数であり，k=n+k_0+2とする。），さらにJacobi記号a=(m_1/n)，および，

【００３７】

【数４５】

$$C = m_1^{2\alpha} g^{r'} \bmod n, \quad D = h^{r'} \bmod n \qquad \cdots (数45)$$

【００３８】

を計算し，(C,D,a)を暗号文として受信者に送信する。

【００３９】

[復号化]

（２）受信者は，自身の秘密鍵（p,q,s,β）を用いて，暗号文(C,D,a)から，

【００４０】

【数４６】

$$\begin{aligned} m_{1,p} &= (CD^s)^{\frac{\beta(p+1)}{4}} \bmod p, \\ m_{1,q} &= (CD^s)^{\frac{\beta(q+1)}{4}} \bmod q \end{aligned} \qquad \cdots (数46)$$

【００４１】

を計算し，ϕ($m_{1,p}$,$m_{1,q}$)，ϕ(-$m_{1,p}$,$m_{1,q}$)，ϕ($m_{1,p}$,-$m_{1,q}$)，ϕ(-$m_{1,p}$,-$m_{1,q}$)のうち，(x/n)=aかつ0<x<2^{k-2}を満たすxをm'_1として計算する。但し，ϕは中国人の剰余定理によるZ/(p)×Z/(q)からZ/(pq)への環同型写像を表す。

【００４２】

さらに，m'_1=s'||t'（s'はm'_1の上位nビット，t'は下位k_0ビット）に対して，

【００４３】

【数４７】

$$m' = \begin{cases} [s' \oplus G(t' \oplus H(s'))]^{n-k_1} & \text{if } [s' \oplus G(t' \oplus H(s'))]_{k_1} = 0^{k_1} \\ * & \text{otherwise} \end{cases} \qquad \cdots (数47)$$

【００４４】

を計算し，これを復号化結果とする（但し，$[a]^n$および$[a]_n$はそれぞれaの上位

および下位nビットを表す。）

【００４５】

【発明の実施の形態】

以下，図面を用いて，本発明の実施例について説明する。

【００４６】

図１は，本発明の実施例のシステム構成を示す図である。このシステムは，送信者側装置100と受信者側装置200から構成されている。さらに，送信者側装置100と受信者側装置200は通信回線300で接続されている。

【００４７】

図２は，実施例における送信者側装置100の内部構成を示す。送信者側装置100は，乱数生成手段101，べき乗算手段102，演算手段103，剰余演算手段104，メモリ105，通信装置106，を備えている。

【００４８】

図３は，実施例における受信者側装置200の内部構成を示す。受信者側装置200は，鍵生成手段201，べき乗算手段202，剰余演算手段203，演算手段204，メモリ205，通信装置206，を備えている。

【００４９】

図４は，実施例２の概要を示す図である。

【００５０】

図５は，実施例３の概要を示す図である。

【００５１】

図６は，実施例４の概要を示す図である。

【００５２】

図７は，実施例５の概要を示す図である。

【００５３】

図８は，本発明の実施例による方式と代表的な実用的公開鍵暗号方式との効率性（モジュラー積の個数）および安全性（IND-CCA2であるか）の比較を表す図である。図８における比較では，本発明の方式においてd=3とした。また，本発明の方式における括弧の中の数字は前処理が可能である場合において前処理を行っ

た結果である。

【００５４】

（実施例１）

本発明の実施例として，まず，選択平文攻撃に対して一方向（OW-CPA）であり，かつ選択平文攻撃に対して強秘匿（IND-CPA）である公開鍵暗号方法について説明する。

【００５５】

鍵生成のステップとして，

【００５６】

【数４８】

- p, q：素数，　$p \equiv 3 \pmod 4$, $q \equiv 3 \pmod 4$
- $s \in \mathbb{Z}$，　$gh^s \equiv 1 \pmod{pq}$

・・・(数４８)

【００５７】

なる秘密鍵（p,q,s）を作成し，さらに，

【００５８】

【数４９】

- $\alpha, g, h, k, l \in \mathbb{Z}$　$(0 < g, h < n)$
- $n = p^d q$　　(d は奇数)

・・・(数４９)

【００５９】

なる公開鍵（n,g,h,k,l）を作成する（但し，kはpqのビット長）。

【００６０】

（１）送信者は，平文m($0<m<2^{k-2}$)および乱数r（$0 \leqq r \leqq l$）に対して，

【００６１】

【数５０】

$$C = m^2 g^r \bmod n, \quad D = h^r \bmod n$$

・・・(数５０)

【００６２】

を計算する，さらにJacobi記号a=(m/n)を計算し，(C,D,a)を暗号文として前記受信者に送信する。

【００６３】

（２）受信者は，自身の秘密鍵（p,q,s）を用いて，暗号文(C,D,a)から，

【００６４】

【数５１】

$$m_{1,p} = (CD^s)^{\frac{(p+1)}{4}} \bmod p, \qquad \cdots(数51)$$
$$m_{1,q} = (CD^s)^{\frac{(q+1)}{4}} \bmod q$$

【００６５】

を計算し，$\phi(m_{1,p},m_{1,q})$，$\phi(-m_{1,p},m_{1,q})$，$\phi(m_{1,p},-m_{1,q})$，$\phi(-m_{1,p},-m_{1,q})$のうち，(x/n)=aかつ$0<x<2^{k-2}$を満たすxを平文mとする（但し，ϕは中国人の剰余定理によるZ/(p)×Z/(q)からZ/(pq)への環同型写像を表す。）。

【００６６】

この方法では，Jacobi記号aを暗号文の一部としており，これにより復号一意性が得られ，処理の高速化が可能となる。

【００６７】

上記公開鍵暗号方法をさらに選択暗号文攻撃に対して強秘匿（IND-CCA2）になるように変換したものを以下の各実施例にて示す。

【００６８】

（実施例２）

本実施例は，メッセージの送信者であるＡが受信者であるＢに対して，送信データｍを暗号通信によって送信する場合について説明する。

【００６９】

図１は，本実施例のシステム構成を示す。また，図２は，本実施例の概要を示す。

【００７０】

１．鍵生成処理

受信者Ｂは，予め，受信者側装置200内の鍵生成手段201を用いて，

【００７１】

【数５２】

- p, q：素数，$p \equiv 3 \pmod 4$, $q \equiv 3 \pmod 4$
- $\beta \in \mathbb{Z}$，$\alpha\beta \equiv 1 \pmod{\mathrm{lcm}(p-1, q-1)}$

・・・(数５２)

【００７２】

なる秘密情報（p,q,β）を作成し，

【００７３】

【数５３】

- $\alpha, k \in \mathbb{Z}$
- $n = p^d q$　　(d は奇数)

・・・(数５３)

【００７４】

なる公開情報（n,k,α）を作成し（但し，ｋはｐｑのビット長を表す。），公開情報を通信回線300などを介して出力し，送信者側装置100へ送付するか，または公開する。公開する方法として，例えば第３者（公開情報管理機関）への登録など，周知の方法を用いることが可能である。その他の情報については，メモリ205に格納する。

【００７５】

２．暗復号化処理

（１）送信者Ａは，平文m（$0<m<2^{n-k1}$）に対して，乱数生成手段101，演算手段103を用いて，乱数r（$0<r<2^{k1}$）を選び，

【００７６】

【数５４】

$$m_1 = m0^{k_1} \oplus G(r) \,\|\, r \oplus H(m0^{k_1} \oplus G(r)) \qquad (0 < m_1 < 2^{k-2}) \qquad \text{・・・(数５４)}$$

【００７７】

を計算する。但し，$G: \{0,1\}^{k0} \rightarrow \{0,1\}^{n}$，$H: \{0,1\}^{n} \rightarrow \{0,1\}^{k0}$，は適当なランダム

関数であり，$k=n+k_0+2$とする。

【００７８】

さらに，第3者あるいは受信者Bから上記公開情報を得て，演算手段103，べき乗算手段102，剰余演算手段104を用いて，Jacobi記号$a=(m_1/n)$，および，

【００７９】

【数５５】

$$C = m_1^{2\alpha} \bmod n, \quad \cdots(数55)$$

【００８０】

を計算する。

【００８１】

さらに，暗号文（Ｃ，ａ）を通信装置106を用いて通信回線300を介して受信者Ｂの受信者側装置200に送信する。

【００８２】

（２）受信者Ｂは，保持している上記秘密情報（p,q,β）と，受信者側装置200内のべき乗算手段202，剰余演算手段203，演算手段204を用いて暗号文(C,a)から

【００８３】

【数５６】

$$m_{1,p} = C^{\frac{\beta(p+1)}{4}} \bmod p, \quad m_{1,q} = C^{\frac{\beta(q+1)}{4}} \bmod q \quad \cdots(数56)$$

【００８４】

を計算し，$\phi(m_{1,p},m_{1,q})$，$\phi(-m_{1,p},m_{1,q})$，$\phi(m_{1,p},-m_{1,q})$，$\phi(-m_{1,p},-m_{1,q})$のうち，$(x/n)=a$かつ$0<x<2^{k-2}$を満たすxをm'_1として計算する。但し，ϕは中国人の剰余定理による$Z/(p)\times Z/(q)$から$Z/(pq)$への環同型写像を表す。

【００８５】

さらに，演算手段204を用いて，$m'_1=s'||t'$（s'はm'_1の上位nビット，t'は下

位k_0ビット）に対して，

【００８６】

【数５７】

$$m' = \begin{cases} [s' \oplus G(t' \oplus H(s'))]^{n-k_1} & \text{if } [s' \oplus G(t' \oplus H(s'))]_{k_1} = 0^{k_1} \\ * & \text{otherwise} \end{cases} \quad \cdots (数57)$$

【００８７】

を計算し，これを復号化結果とする（但し，$[a]^n$および$[a]_n$はそれぞれaの上位および下位nビットを表す。）

なお，上記式において、m'=*とは，if以下の条件が成立しないときは，正しい復号結果が得られないものとしてエラーを出力する，あるいは復号化処理を中断するなど，システム構成に依存する処理を行うことを示している。

【００８８】

上記方法を用いれば，適応的選択暗号文攻撃に対して強秘匿であることがnの素因数分解問題の困難性との等価性により証明することができる。

【００８９】

また，本実施例の方法によると，暗号化処理はほぼ２回のモジュラー積を行うのみであり，また，復号化処理においてはnよりも小さいpqの上で行うことにより，従来方法に比べて処理の高速性を実現している。

【００９０】

（実施例３）

本実施例は，実施例１が決定的アルゴリズム（確率暗号ではない）からIND-CCA2となるように変換したものであるのに対して，確率的アルゴリズムからIND-CCA2になるように変換したものである。

【００９１】

１．鍵生成処理

受信者Ｂは，予め，受信者側装置200内の鍵生成手段201を用いて，

【００９２】

【数５８】

- p, q：素数，　$p \equiv 3 \pmod 4$, $q \equiv 3 \pmod 4$
- $s \in \mathbb{Z}$,　$gh^s \equiv 1 \pmod{pq}$　　・・・(数５８)
- $\beta \in \mathbb{Z}$,　$\alpha\beta \equiv 1 \pmod{\mathrm{lcm}(p-1, q-1)}$

【００９３】

なる秘密情報（p,q,s,β）を作成し，

【００９４】

【数５９】

- $\alpha, g, h, k, l \in \mathbb{Z}$　$(0 < g, h < n)$
- $n = p^d q$　　(d は奇数)　　・・・(数５９)

【００９５】

なる公開情報（n,g,h,k,l,α）を作成し（但し，ｋはｐｑのビット長を表す。），公開情報を通信回線300などを介して出力し，送信者側装置100へ送付するか，または公開する。公開する方法として，例えば第３者（公開情報管理機関）への登録など，周知の方法を用いることが可能である。その他の情報については，メモリ205に格納する。

【００９６】

２．暗復号化処理

（１）送信者Ａは，平文m（$0<m<2^{n-k1}$）に対して，乱数生成手段101，演算手段103を用いて，乱数r（$0<r<2^{k1}$）を選び，

【００９７】

【数６０】

$$m_1 = m0^{k_1} \oplus G(r) \,||\, r \oplus H(m0^{k_1} \oplus G(r)) \qquad (0 < m_1 < 2^{k-2}) \qquad \cdots (数６０)$$

【００９８】

を計算する。但し，$G: \{0,1\}^{k0} \rightarrow \{0,1\}^{n}$，$H: \{0,1\}^{n} \rightarrow \{0,1\}^{k0}$，は適当なランダム関数であり，$k=n+k_0+2$とする。

【００９９】

さらに，第3者あるいは受信者Bから上記公開情報を得て，演算手段103，べき乗算手段102，剰余演算手段104を用いて，Jacobi記号$a=(m_1/n)$，および，

【０１００】

【数６１】

$$C = m_1^{2\alpha} g^{r'} \bmod n, \quad D = h^{r'} \bmod n \qquad \cdots (数61)$$

【０１０１】

を計算する。

【０１０２】

さらに，暗号文（C,D,a）を通信装置106を用いて通信回線300を介して受信者Bの受信者側装置200に送信する。

【０１０３】

（２）受信者Bは，保持している上記秘密情報（p,q,s,β）と，受信者側装置200内のべき乗算手段202，剰余演算手段203，演算手段204を用いて暗号文(C,D,a)から，

【０１０４】

【数６２】

$$\begin{aligned} m_{1,p} &= (CD^s)^{\frac{\beta(p+1)}{4}} \bmod p, \\ m_{1,q} &= (CD^s)^{\frac{\beta(q+1)}{4}} \bmod q \end{aligned} \qquad \cdots (数62)$$

【０１０５】

を計算し，$\phi(m_{1,p}, m_{1,q})$，$\phi(-m_{1,p}, m_{1,q})$，$\phi(m_{1,p}, -m_{1,q})$，$\phi(-m_{1,p}, -m_{1,q})$のうち，$(x/n)=a$かつ$0<x<2^{k-2}$を満たすxをm'_1として計算する。但し，ϕは中国人の剰余定理によるZ/(p)×Z/(q)からZ/(pq)への環同型写像を表す。

【０１０６】

さらに，演算手段204を用いて，$m'_1=s'||t'$（s'はm'_1の上位nビット，t'は下位k_0ビット）に対して，

【０１０７】

【数６３】

$$m' = \begin{cases} [s' \oplus G(t' \oplus H(s'))]^{n-k_1} & \text{if } [s' \oplus G(t' \oplus H(s'))]_{k_1} = 0^{k_1} \\ * & \text{otherwise} \end{cases} \quad \cdots (数63)$$

【０１０８】

を計算し，これを復号化結果とする（但し，$[a]^n$および$[a]_n$はそれぞれaの上位および下位nビットを表す。）

本実施例による方法では，nの素因数分解問題よりも困難な問題の困難性を前提として，IND-CCA2であることを示すことができる。

【０１０９】

（実施例４）

上記実施例３において，

【０１１０】

【数６４】

$$g^{r'} \bmod n, \quad h^{r'} \bmod n \quad \cdots (数64)$$

【０１１１】

の計算は，暗号化対象である送信データmに関係しないため，前処理が可能である。すなわち，これらの計算を前処理として行い，その結果をコンピュータAの記憶手段（メモリ，二次記憶装置など）に保存して，その値を読み出して用いることにより，暗号化時間を大幅に短縮する事ができる。

【０１１２】

前処理を行うと，送信データmを用いた処理のモジュラー積の個数は1個となるため，暗号化時間を大幅に短縮することが可能となる。

【０１１３】

（実施例５）

本実施例は，実施例３の変形例である。

【０１１４】

１．鍵生成処理

受信者Ｂは，予め，受信者側装置200内の鍵生成手段201を用いて，

【０１１５】

【数６５】

- p, q：素数，$p \equiv 3 \pmod 4$, $q \equiv 3 \pmod 4$
- $s \in \mathbb{Z}$，$gh^s \equiv 1 \pmod{pq}$
- $\beta \in \mathbb{Z}$，$\alpha\beta \equiv 1 \pmod{\mathrm{lcm}(p-1, q-1)}$

・・・(数６５)

【０１１６】

なる秘密情報（p,q,s,β）を作成し，

【０１１７】

【数６６】

- $\alpha, g, h, k, l \in \mathbb{Z}$　$(0 < g, h < n)$
- $n = p^d q$　　(d は奇数)

・・・(数６６)

【０１１８】

なる公開情報（n,g,h,k,l,α）を作成し（但し，ｋはｐｑのビット長を表す。），公開情報を通信回線300などを介して出力し，送信者側装置100へ送付するか，または公開する。公開する方法として，例えば第３者（公開情報管理機関）への登録など，周知の方法を用いることが可能である。その他の情報については，メモリ205に格納する。

【０１１９】

２．暗復号化処理

（１）送信者Ａは，平文ｍ（$0<m<2^n$）に対して，乱数生成手段101，演算手段103

を用いて，乱数r（$0<r<2^{k0}$）を選び，

【０１２０】

【数６７】

$$m_1 = m \oplus G(r) \,||\, r \oplus H(m \oplus G(r)) \qquad (0 < m_1 < 2^{k-2}) \qquad \cdots (数67)$$

【０１２１】

を計算する。但し，$G: \{0,1\}^{k0} \rightarrow \{0,1\}^{n}$，$H: \{0,1\}^{n} \rightarrow \{0,1\}^{k0}$，は適当なランダム関数であり，$k=n+k_0+2$とする。

【０１２２】

さらに，第3者あるいは受信者Bから上記公開情報を得て，演算手段103，べき乗算手段102，剰余演算手段104を用いて，Jacobi記号$a=(m_1/n)$，および，

【０１２３】

【数６８】

$$C = m_1^{2\alpha} g^{F(m_1)} \bmod n, \quad D = h^{F(m_1)} \bmod n \qquad \cdots (数68)$$

【０１２４】

を計算する。但し，$F: \{0,1\}^{n+k0} \rightarrow \{0,1\}^{l}$は適当なランダム関数。

【０１２５】

さらに，暗号文（C,D,a）を通信装置106を用いて通信回線300を介して受信者Ｂの受信者側装置200に送信する。

【０１２６】

（２）受信者Ｂは，保持している上記秘密情報（p,q,s,β）と，受信者側装置200内のべき乗算手段202，剰余演算手段203，演算手段204を用いて暗号文(C,D,a)から，

【０１２７】

【数６９】

$$\begin{aligned} m_{1,p} &= (CD^s)^{\frac{\beta(p+1)}{4}} \bmod p, \\ m_{1,q} &= (CD^s)^{\frac{\beta(q+1)}{4}} \bmod q \end{aligned} \qquad \cdots (数69)$$

【０１２８】

を計算し，$\phi(m_{1,p},m_{1,q})$，$\phi(-m_{1,p},m_{1,q})$，$\phi(m_{1,p},-m_{1,q})$，$\phi(-m_{1,p},-m_{1,q})$のうち，(x/n)=aかつ$0<x<2^{k-2}$を満たすxをm'_1として計算する。但し，ϕは中国人の剰余定理によるZ/(p)×Z/(q)からZ/(pq)への環同型写像を表す。

【０１２９】

さらに，演算手段204を用いて，$m'_1=s'||t'$（s'はm'_1の上位nビット，t'は下位k_0ビット）に対して，

【０１３０】

【数７０】

$$m' = \begin{cases} s' \oplus G(t' \oplus H(s')) & \text{if } (C,D) = (C',D') \\ * & \text{otherwise} \end{cases} \quad \cdots \text{(数70)}$$

【０１３１】

を計算し，これを復号化結果とする。但し，

【０１３２】

【数７１】

$$C' = m_1'^2 g^{F(m_1')} \bmod n, \quad D' = h^{F(m_1')} \bmod n \quad \cdots \text{(数71)}$$

【０１３３】

であり，$[a]^n$および$[a]_n$はそれぞれaの上位および下位nビットを表す。

【０１３４】

本実施例による方法では，nの素因数分解問題よりも困難な問題の困難性を前提として，IND-CCA2であることを示すことができる。

【０１３５】

また，本実施例の方法においては，実施例３の方法に比べて，平文を長くとることが可能である。

【０１３６】

（実施例６）

本実施例は，実施例３の変形例である。

【０１３７】

１．鍵生成処理

受信者Ｂは，予め，受信者側装置200内の鍵生成手段201を用いて，

【０１３８】

【数７２】

- p, q：素数，$p \equiv 3 \pmod 4$, $q \equiv 3 \pmod 4$
- $s \in \mathbb{Z}$，$gh^s \equiv 1 \pmod{pq}$ ・・・(数72)
- $\beta \in \mathbb{Z}$，$\alpha\beta \equiv 1 \pmod{\mathrm{lcm}(p-1, q-1)}$

【０１３９】

なる秘密情報（p,q,s,β）を作成し，

【０１４０】

【数７３】

- $\alpha, g, h, k, l \in \mathbb{Z}$　$(0 < g, h < n)$ ・・・(数73)
- $n = p^d q$　　(d は奇数)

【０１４１】

なる公開情報（n,g,h,k,l,α）を作成し（但し，ｋはｐｑのビット長を表す。），公開情報を通信回線300などを介して出力し，送信者側装置100へ送付するか，または公開する。公開する方法として，例えば第３者（公開情報管理機関）への登録など，周知の方法を用いることが可能である。その他の情報については，メモリ205に格納する。

【０１４２】

２．暗復号化処理

（１）送信者Ａは，平文m（$0<m<2^n$）に対して，乱数生成手段101，演算手段103を用いて，乱数r（$0<r<2^{k0}$）を選び，

【０１４３】

【数７４】

$$m_1 = m \| r \qquad \cdots (数74)$$

【０１４４】

を計算する。但し，F: $\{0,1\}^{n+k0} \rightarrow \{0,1\}^{l}$は適当なランダム関数であり，$k=n+k_0+2$とする。

【０１４５】

さらに，第3者あるいは受信者Bから上記公開情報を得て，演算手段103，べき乗算手段102，剰余演算手段104を用いて，Jacobi記号$a=(m_1/n)$，および，

【０１４６】

【数７５】

$$C = m_1^{2\alpha} g^{F(m_1)} \bmod n, \quad D = h^{F(m_1)} \bmod n \qquad \cdots (数75)$$

【０１４７】

を計算する。

【０１４８】

さらに，暗号文（C,D,a）を通信装置106を用いて通信回線300を介して受信者Ｂの受信者側装置200に送信する。

【０１４９】

（２）受信者Ｂは，保持している上記秘密情報（p,q,s,β）と，受信者側装置200内のべき乗算手段202，剰余演算手段203，演算手段204を用いて暗号文(C,D,a)から，

【０１５０】

【数７６】

$$m_{1,p} = (CD^s)^{\frac{\beta(p+1)}{4}} \bmod p, \quad m_{1,q} = (CD^s)^{\frac{\beta(q+1)}{4}} \bmod q \qquad \cdots(数76)$$

【０１５１】

を計算し，$\phi(m_{1,p}, m_{1,q})$, $\phi(-m_{1,p}, m_{1,q})$, $\phi(m_{1,p}, -m_{1,q})$, $\phi(-m_{1,p}, -m_{1,q})$のうち，(x/n)=aかつ$0<x<2^{k-2}$を満たすxをm'_1として計算する。但し，ϕは中国人の剰余定理によるZ/(p)×Z/(q)からZ/(pq)への環同型写像を表す。

【０１５２】

さらに，演算手段204を用いて，

【０１５３】

【数７７】

$$m' = \begin{cases} [m'_1]^{k_0} & \text{if } (C,D) = (C',D') \\ * & \text{otherwise} \end{cases} \qquad \cdots(数77)$$

【０１５４】

を計算し，これを復号化結果とする。但し，

【０１５５】

【数７８】

$$C' = m_1'^{2\alpha} g^{F(m'_1)} \bmod n, \quad D' = h^{F(m'_1)} \bmod n \qquad \cdots(数78)$$

【０１５６】

であり，$[a]^n$および$[a]_n$はそれぞれaの上位および下位nビットを表す。

【０１５７】

本実施例による方法では，「条件付きDiffie-Hellman問題」の困難性を前提として，IND-CCA2であることを示すことができる。

【０１５８】

また，本実施例の方法においては，実施例３の方法に比べて，平文を長くとることが可能である。

【０１５９】

（実施例７）

本実施例は，実施例５および実施例６において，受信者側の計算効率を高めるための復号化方法について述べる。

【０１６０】

受信者は，受信者側装置200内のべき乗算手段202，剰余演算手段203，演算手段204を用いて，

【０１６１】

【数７９】

$$C'_p = m_1'^{2\alpha} g^{F(m_1')} \bmod p^d, \qquad C'_q = m_1'^{2\alpha} g^{F(m_1')} \bmod q$$
$$D'_p = h^{F(m_1')} \bmod p^d, \qquad D'_q = h^{F(m_1')} \bmod q \qquad \cdots (数79)$$

【０１６２】

を計算し，さらに

【０１６３】

【数８０】

$$C \equiv C'_p \pmod{p^d}, \quad C \equiv C'_q \pmod{q}, \qquad \cdots (数80)$$
$$D \equiv D'_p \pmod{p^d}, \quad D \equiv D'_q \pmod{q}$$

【０１６４】

により，(C,D)=(C',D')を検査する。

【０１６５】

（実施例８）

本実施例は，選択平文攻撃に対して強秘匿，すなわち IND-CPA，である公開鍵暗号方法について述べる。

【０１６６】

１．鍵生成処理

受信者Ｂは，予め，受信者側装置200内の鍵生成手段201を用いて，

【０１６７】

【数８１】

- p, q：素数，$p \equiv 3 \pmod 4$, $q \equiv 3 \pmod 4$
- $s \in \mathbb{Z}$，$gh^s \equiv 1 \pmod{pq}$
- $\beta \in \mathbb{Z}$，$\alpha\beta \equiv 1 \pmod{\mathrm{lcm}(p-1, q-1)}$

・・・(数８１)

【０１６８】

なる秘密情報（p,q,s,β）を作成し，

【０１６９】

【数８２】

- $\alpha, g, h, k, l \in \mathbb{Z}$　$(0 < g, h < n)$
- $n = p^d q$　　(d は奇数)

・・・(数８２)

【０１７０】

なる公開情報（n,g,h,k,l,α）を作成し（但し，ｋはｐｑのビット長を表す。），公開情報を通信回線300などを介して出力し，送信者側装置100へ送付するか，または公開する。公開する方法として，例えば第３者（公開情報管理機関）への登録など，周知の方法を用いることが可能である。その他の情報については，メモリ205に格納する。

【０１７１】

２．暗復号化処理

（１）送信者Ａは，平文m（$0<m<2^{k-2}$）に対して，乱数生成手段101，演算手段103を用いて，乱数r（0<r<l）を選び，

【０１７２】

【数８３】

$$C = m^{2\alpha} g^{r'} \bmod n, \quad D = h^{r'} \bmod n \qquad \cdots (数83)$$

【０１７３】

を計算する。

【０１７４】

さらに，第3者あるいは受信者Bから上記公開情報を得て，演算手段103，べき乗算手段102，剰余演算手段104を用いて，Jacobi記号a=(m/n)を計算する。

【０１７５】

さらに，暗号文（C,D,a）を通信装置106を用いて通信回線300を介して受信者Ｂの受信者側装置200に送信する。

【０１７６】

（２）受信者Ｂは，保持している上記秘密情報（p,q,s,β）と，受信者側装置200内のべき乗算手段202，剰余演算手段203，演算手段204を用いて暗号文(C,D,a)から，

【０１７７】

【数８４】

$$\begin{aligned} m_{1,p} &= (CD^s)^{\frac{\beta(p+1)}{4}} \bmod p, \\ m_{1,q} &= (CD^s)^{\frac{\beta(q+1)}{4}} \bmod q \end{aligned} \qquad \cdots (数84)$$

【０１７８】

を計算し，$\phi(m_{1,p}, m_{1,q})$，$\phi(-m_{1,p}, m_{1,q})$，$\phi(m_{1,p}, -m_{1,q})$，$\phi(-m_{1,p}, -m_{1,q})$のうち，(x/n)=aかつ$0<x<2^{k-2}$を満たすxを平文mとして計算する。但し，ϕは中国人の剰余定理によるZ/(p)×Z/(q)からZ/(pq)への環同型写像を表す。

【０１７９】

本実施例による方法では，nの素因数分解問題よりも困難な問題の困難性を前

提として完全解読が不可能なこと，さらに「条件付きのDiffie-Hellman決定問題」の困難性を前提として強秘匿であることを示すことができる。ここで，「条件付きのDiffie-Hellman決定問題」とは，確率分布

【０１８０】

【数８５】

$$D_0 : (h, g, h^r, g^r), \quad 0 \le r \le l,$$
$$D_1 : (h, g, h^r, Xg^r), \quad X = (x/x')^{2\alpha} \bmod n, \ 0 < x, x' < 2^{k-2} \qquad \cdots (数85)$$

【０１８１】

において，D_0またはD_1からの任意のシーケンスに対して，いずれからのものであるかを言い当てる問題である。

【０１８２】

以上，実施例では，送信者と受信者が各々の装置を利用して暗号通信を行うという一般形で述べたが，具体的には様々なシステムに適用される。

【０１８３】

例えば，電子ショッピングシステムでは，送信者はユーザであり，送信者側装置はパソコンなどの計算機であり，受信者は小売店，受信者側装置はパソコンなどの計算機となる。このとき，ユーザの商品等の注文書は共通鍵暗号で暗号化されることが多く，その際の暗号化鍵を本実施例による方法により暗号化されて小売店側装置に送信される。

【０１８４】

また，電子メールシステムでは，各々の装置はパソコンなどの計算機であり，送信者のメッセージは共通鍵暗号で暗号化されることが多く，その際の暗号化鍵を本実施例による方法により暗号化されて受信者の計算機に送信される。

【０１８５】

その他にも，従来の公開鍵暗号が使われている様々なシステムに適用することが可能である。

【０１８６】

なお，本実施例における各計算は，CPUがメモリ内の各プログラムを実行することにより行われるものとして説明したが，プログラムだけではなく，いずれかがハードウエア化された演算装置であって，他の演算装置や，CPUと，データのやりとりを行うものであっても良い。

【０１８７】

【発明の効果】

本発明によれば，最も強力な攻撃法である適応的選択暗号文攻撃に対しても安全であり，さらに，高速処理が可能な，公開鍵暗号方法と，その応用装置，システムを実現することができる。

【図面の簡単な説明】

【図１】

本発明の実施例のシステム構成を示す図である。

【図２】

本発明の実施例における送信者側装置の内部構成を示す図である。

【図３】

本発明の実施例における受信者側装置の内部構成を示す図である。

【図４】

本発明の実施例２の概要を示す図である。

【図５】

本発明の実施例３の概要を示す図である。

【図６】

本発明の実施例４の概要を示す図である。

【図７】

本発明の実施例５の概要を示す図である。

【図８】

本発明の実施例による方式と代表的な実用的公開鍵暗号方式との効率性（モジュラー積の個数）の比較を表す図である。

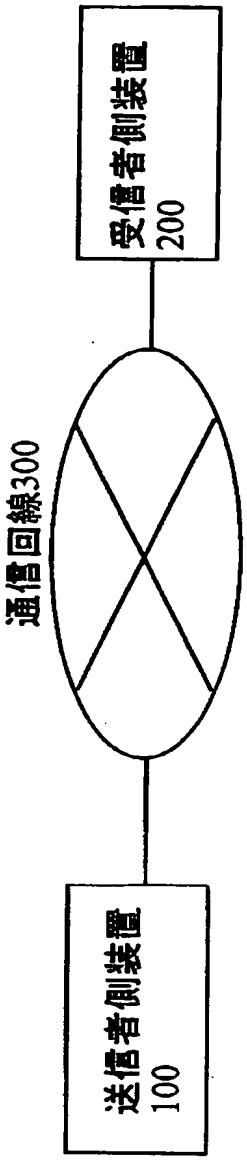
【符号の説明】

１００…送信者側装置，１０１…送信者側装置１００内の乱数生成手段，１０２…送信者側装置１００内のべき乗算手段，１０３…送信者側装置１００内の演算手段，１０４…送信者側装置１００内の剰余演算手段，１０５…送信者側装置１００内のメモリ，１０６…送信者側装置１００内の通信装置，２００…受信者側装置，２０１…受信者側装置２００内の鍵生成手段，２０２…受信者側装置２００内のべき乗算手段，２０３…受信者側装置２００内の剰余演算手段，２０４…受信者側装置２００内の演算手段，２０５…受信者側装置２００内のメモリ，２０６…受信者側装置２００内の通信装置。。

【書類名】　図面

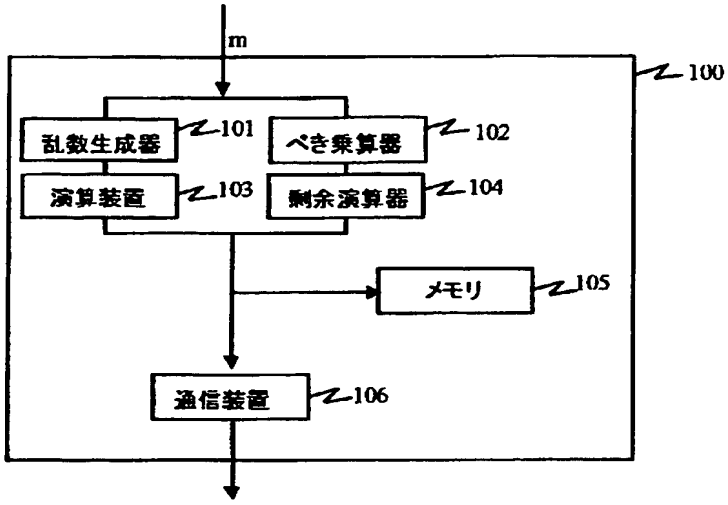
【図１】

図１



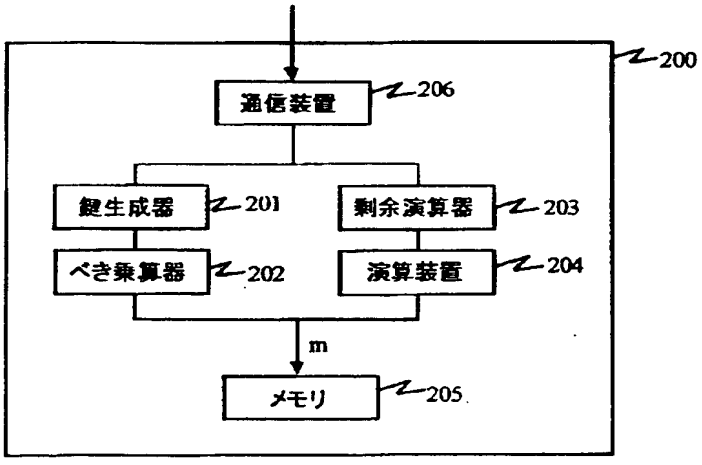
【図２】

図2


m
100
乱数生成器
101
べき乗算器
102
演算装置
103
剰余演算器
104
メモリ
105
通信装置
106

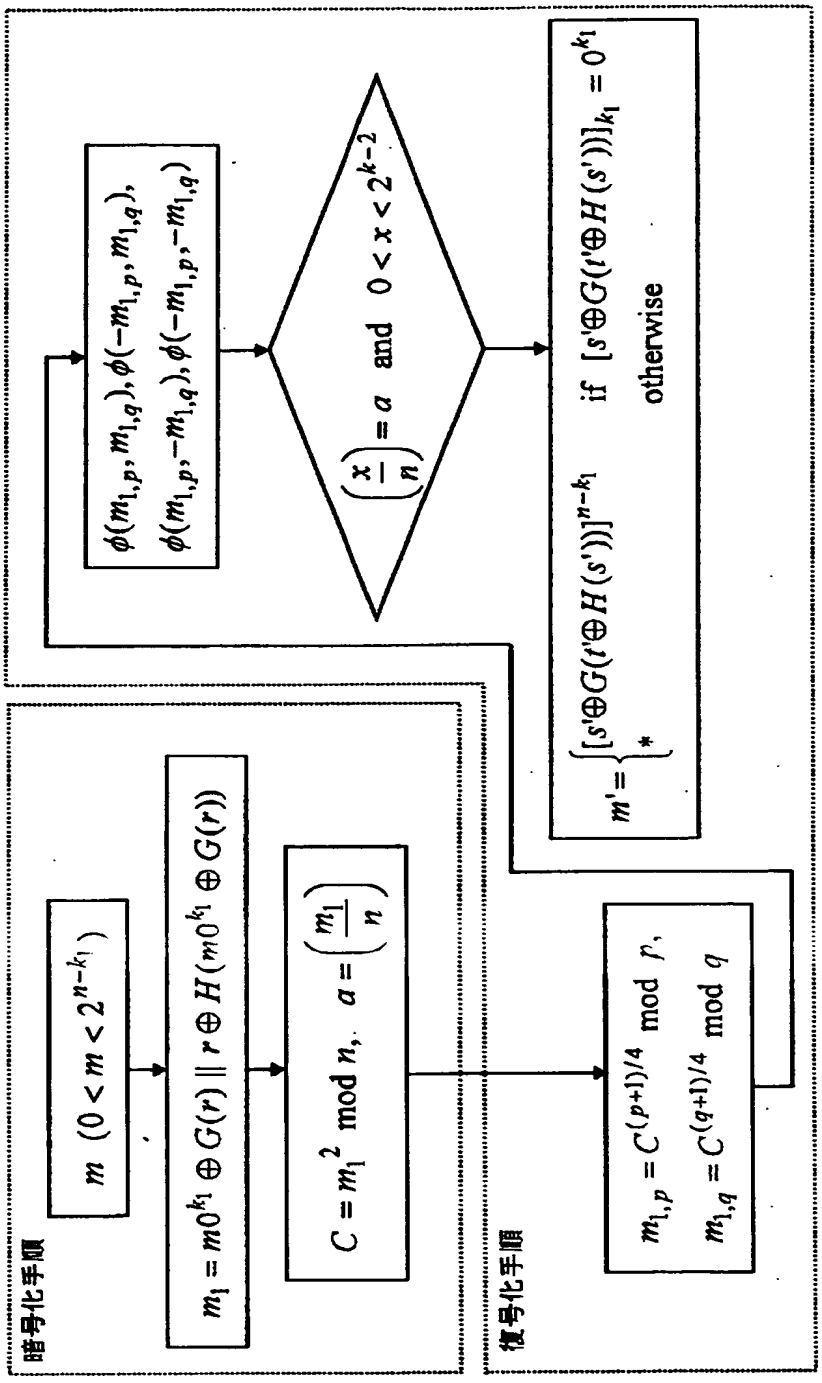
【図３】

図３


200
通信装置
206
鍵生成器
201
剰余演算器
203
べき乗算器
202
演算装置
204
m
メモリ
205

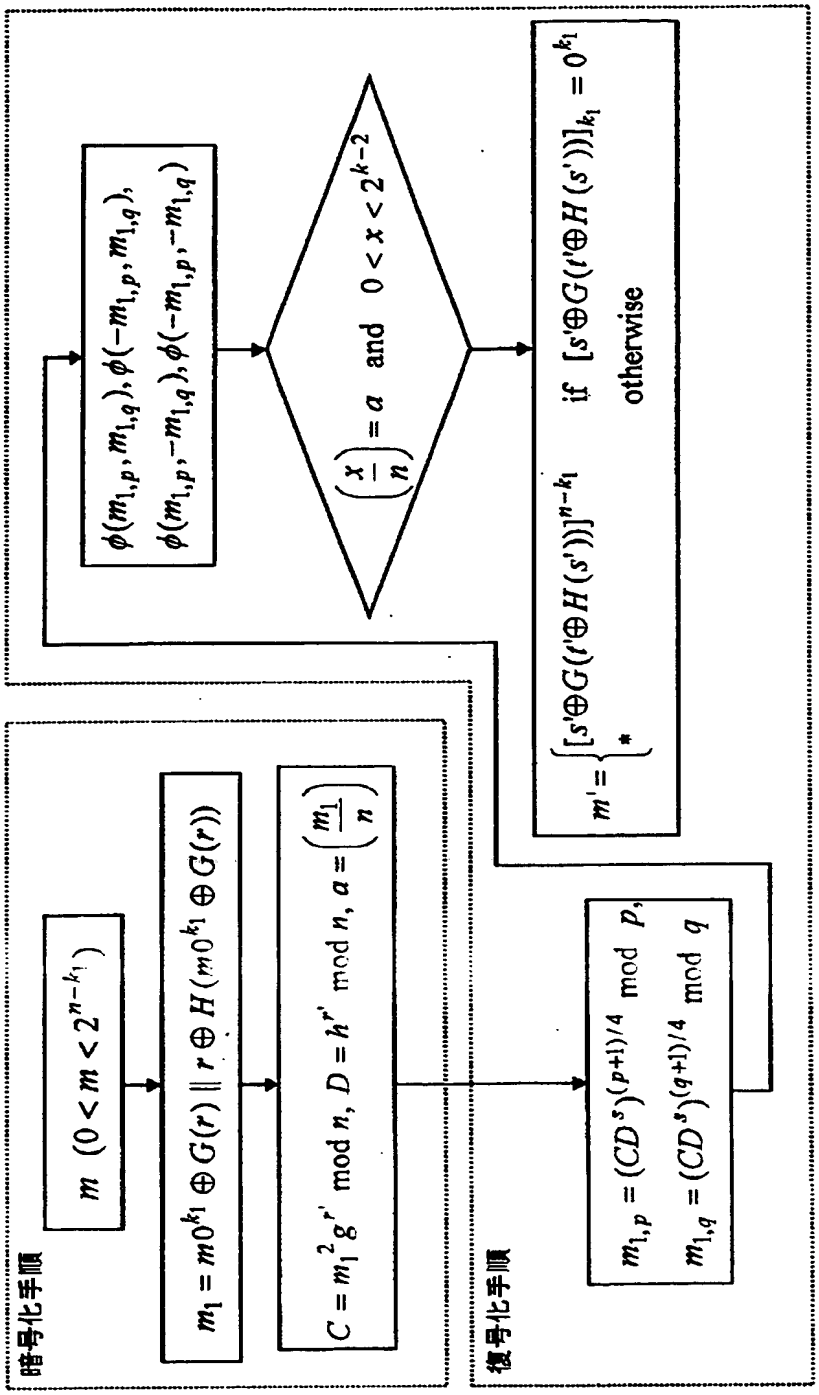
【図４】

図 4


暗号化手順
$m \quad (0 < m < 2^{n-k_1})$
$m_1 = m0^{k_1} \oplus G(r) \| r \oplus H(m0^{k_1} \oplus G(r))$
$C = m_1^2 \bmod n, \quad a = \left(\frac{m_1}{n}\right)$
復号化手順
$m_{1,p} = C^{(p+1)/4} \bmod p,$
$m_{1,q} = C^{(q+1)/4} \bmod q$
$\phi(m_{1,p}, m_{1,q}), \phi(-m_{1,p}, m_{1,q}),$
$\phi(m_{1,p}, -m_{1,q}), \phi(-m_{1,p}, -m_{1,q})$
$\left(\frac{x}{n}\right) = a$ and $0 < x < 2^{k-2}$
$m' = \begin{cases} [s' \oplus G(t' \oplus H(s'))]_{k_1} = 0^{k_1} & \text{if } [s' \oplus G(t' \oplus H(s'))]^{n-k_1} \\ * & \text{otherwise} \end{cases}$

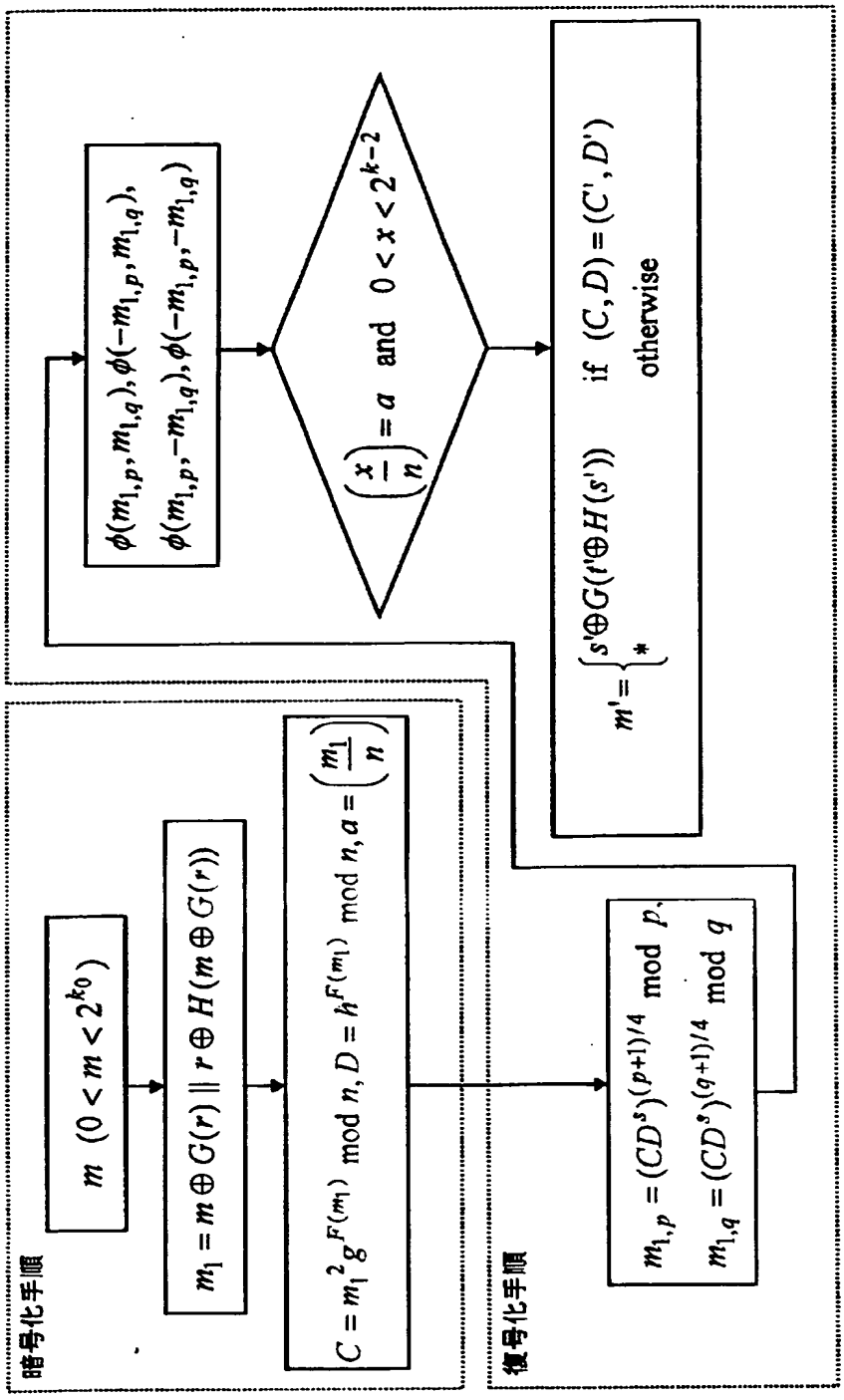
【図５】

図 5


暗号化手順
$m \quad (0 < m < 2^{n-k_1})$
$m_1 = m0^{k_1} \oplus G(r) \| r \oplus H(m0^{k_1} \oplus G(r))$
$C = m_1^2 g^{r'} \bmod n,\ D = h^{r'} \bmod n,\ a = \left(\frac{m_1}{n}\right)$
$\phi(m_{1,p}, m_{1,q}), \phi(-m_{1,p}, m_{1,q}),$
$\phi(m_{1,p}, -m_{1,q}), \phi(-m_{1,p}, -m_{1,q})$
$\left(\frac{x}{n}\right) = a$ and $0 < x < 2^{k-2}$
$m' = \begin{cases} [s' \oplus G(t' \oplus H(s'))]^{n-k_1} & \text{if } [s' \oplus G(t' \oplus H(s'))]_{k_1} = 0^{k_1} \\ * & \text{otherwise} \end{cases}$
復号化手順
$m_{1,p} = (CD^s)^{(p+1)/4} \bmod p,$
$m_{1,q} = (CD^s)^{(q+1)/4} \bmod q$

【図６】

図 6


暗号化手順
$m \quad (0 < m < 2^{k_0})$
$m_1 = m \oplus G(r) \| r \oplus H(m \oplus G(r))$
$C = m_1^2 g^{F(m_1)} \bmod n, D = h^{F(m_1)} \bmod n, a = \left(\frac{m_1}{n}\right)$
復号化手順
$m_{1,p} = (CD^s)^{(p+1)/4} \bmod p$
$m_{1,q} = (CD^s)^{(q+1)/4} \bmod q$
$\phi(m_{1,p}, m_{1,q}), \phi(-m_{1,p}, m_{1,q}),$
$\phi(m_{1,p}, -m_{1,q}), \phi(-m_{1,p}, -m_{1,q})$
$\left(\frac{x}{n}\right) = a$ and $0 < x < 2^{k-2}$
$m' = \begin{cases} s' \oplus G(t' \oplus H(s')) & \text{if } (C, D) = (C', D') \\ * & \text{otherwise} \end{cases}$

【図７】

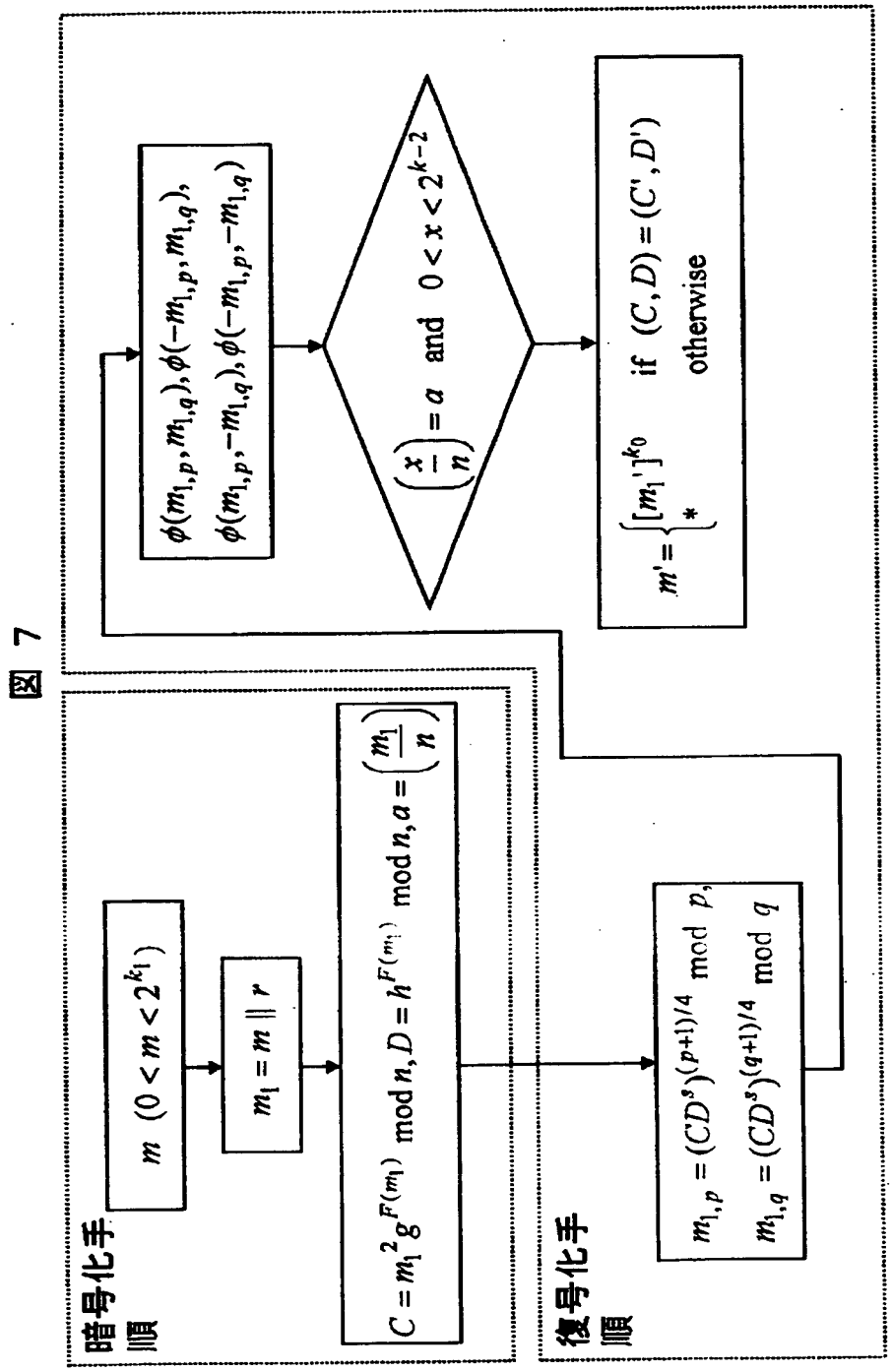

暗号化手順
$m \ (0 < m < 2^{k_1})$
$m_1 = m \| r$
$C = m_1^2 g^{F(m_1)} \bmod n, D = h^{F(m_1)} \bmod n, a = \left(\frac{m_1}{n}\right)$
復号化手順
$m_{1,p} = (CD^5)^{(p+1)/4} \bmod p,$
$m_{1,q} = (CD^5)^{(q+1)/4} \bmod q$
$\phi(m_{1,p}, m_{1,q}), \phi(-m_{1,p}, m_{1,q}),$
$\phi(m_{1,p}, -m_{1,q}), \phi(-m_{1,p}, -m_{1,q})$
$\left(\frac{x}{n}\right) = a$ and $0 < x < 2^{k-2}$
$m' = \begin{cases} [m_1']^{k_0} & \text{if } (C,D) = (C',D') \\ * & \text{otherwise} \end{cases}$

図 7

【図８】

図８

	暗号化	復号化	IND-CCA2
RSA	約 2～1500	約 400	No
ElGamal暗号	約 3000	約 1500	No
楕円暗号	約 120	約 60	No
OAEP	約 2～1500	約 400	Yes
本発明の方式	約 2～200	約 60～210	Yes

【書類名】　要約書

【要約】

【課題】

受信者の公開鍵を用いて，送信データを暗号化する公開鍵暗号による暗号通信方法であって，適応的暗号文攻撃に対して強秘匿であることの証明により安全性を保証することができ，かつ，暗復号化のための計算において効率性の高い処理ができる公開鍵暗号方法および装置を提供する。

【解決手段】

選択平文攻撃に対する一方向性（OW-CPA）を素因数分解問題よりも困難な問題の難しさを前提として保証可能な公開鍵暗号方法に対して，平文に乱数情報と（理想的）ランダム関数へのアクセスの結果から排他的論理和および連接（データの単純な接続）の変換（以下，変換Conと呼ぶ）を行うことにより，適応的選択暗号文攻撃に対する強秘匿性（IND-CCA2）を，素因数分解問題の困難性以上の暗号学的仮定により保証する。

【選択図】　図１

出　願　人　履　歴　情　報

識別番号　〔０００００５１０８〕

１．変更年月日　１９９０年　８月３１日
［変更理由］　新規登録
住　所　東京都千代田区神田駿河台４丁目６番地
氏　名　株式会社日立製作所